



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/068,776	02/06/2002	Michael Neuman	2696-001	7550

22208 7590 04/19/2007  
ROBERTS, MARDULA & WERTHEIM, LLC  
11800 SUNRISE VALLEY DRIVE  
SUITE 1000  
RESTON, VA 20191

EXAMINER
----------

LANIER, BENJAMIN E

ART UNIT	PAPER NUMBER
----------	--------------

2132

SHORTENED STATUTORY PERIOD OF RESPONSE	MAIL DATE	DELIVERY MODE
3 MONTHS	04/19/2007	PAPER

**Please find below and/or attached an Office communication concerning this application or proceeding.**

If NO period for reply is specified above, the maximum statutory period will apply and will expire 6 MONTHS from the mailing date of this communication.

**Office Action Summary**

Application No.

10/068,776

Applicant(s)

NEUMAN ET AL.

Examiner

Benjamin E. Lanier

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 30 March 2007.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims**

- 4) ☒ Claim(s) 1-22,35 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-22 and 35 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

**Priority under 35 U.S.C. § 119**

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
1. ☐ Certified copies of the priority documents have been received.
  2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

\* See the attached detailed Office action for a list of the certified copies not received.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date \_\_\_\_\_
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date \_\_\_\_\_
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_

## **DETAILED ACTION**

### ***Response to Amendment***

1. Applicant's amendment filed 30 March 2007 amends claim 1 and cancels claims 23-34 and 36. Applicant's amendment has been fully considered and entered.

### ***Response to Arguments***

2. Applicant's argument that He does not disclose a separate interface for each node in the network is persuasive, however, upon further consideration, a new ground(s) of rejection is made in view of Sun, U.S. Publication No. 2002/0152373.

### ***Claim Rejections - 35 USC § 102***

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1, 7, 9, 11 are rejected under 35 U.S.C. 102(e) as being anticipated by Sun, U.S. Publication No. 2002/0152373. Referring to claims 1, 11, Sun discloses a tunnel interface for securing traffic over a network wherein each node in the network has a router between itself and the network (Figures 4 & 14), which meets the limitation of providing an intelligent network interface between a network and each node on the network. The routers encrypt and decrypt traffic between network nodes (Figure 14 & [0115]), which meets the limitation of encrypting and decrypting critical data transmissions over the network using said intelligent network interfaces. The SMS provides IPSec public/private key generation for the nodes in the network

Art Unit: 2132

[[0041]], which meets the limitation of centrally managing keys and algorithms used by said intelligent network interfaces for encrypting and decrypting critical data transmissions over the network with a central management console.

Referring to claim 7, Sun discloses that the SMS negotiates a channel between two nodes having unique identifiers ([0060]), which meets the limitation of a first intelligent network interface associated with a first client sending a request to the central management console with the identifying information about a connection that the first client wishes to send to a second client, said information including protocol, distinguished name, service, and header information. Security configurations and policy configurations are maintained by the SMS (See table 1, page 7), which meets the limitation of said CMC reviewing said connection against a network policy and determining denial or allowance of said connection and, upon allowance, further determining encryption algorithm, authentication required, keys for connection, if the connection should be redirected to another node, and if the connection needs to be translated. The SMS provides IPsec public/private key generation for the nodes in the network ([0041]), which meets the limitation of said CMC sending a connection determination, including encryption and authentication algorithm(s), key(s), and any translation servlets required to said first intelligent network interface. While Sun does not expressly disclose authentication or authentication algorithms, these are known to be inherent elements of the IPsec protocol. The authentication header is standard to the IPsec protocol and includes the authentication information mentioned above. The IPsec communications are initialized by a first node ([0060]), which meets the limitation of said first intelligent network interface initiating said connection with a second intelligent network interface associated with said second client. The limitation of sending encrypted connection

Art Unit: 2132

information with authentication is inherent to IPSec. The SMS negotiates a logical ID to have a channel going between the two nodes ([0060]), which meets the limitation of said second intelligent network interface querying said CMC. The limitation of querying with said encrypted connection information received from said first intelligent network interface, including a security parameters index (SPI) for said connection that uniquely identifies said connection between said first and second intelligent network interfaces is inherent to IPSec.

Referring to claim 9, Sun discloses that the SMS software is included within the IP system (Figure 2, element 221 within element 201). Figure 4 shows two IP systems (elements 201-1 & 201-2), which meets the limitation of providing a plurality of CMCs on said network in a hierarchical configuration because there is more than one IP system containing an SMS and they are in a configuration that can be considered hierarchical.

***Claim Rejections - 35 USC § 103***

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

6. The factual inquiries set forth in *Graham v. John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

7. Claims 2-6, 22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sun, U.S. Publication No. 2002/0152373, in view of Lilja, U.S. Patent No. 6,789,157. Referring to claims 2, 3, Sun discloses that the router encrypts IP protocol packets to create IPsec protocol packets ([0040] & [0043] & [0045] & [0115]), which meets the limitation of each intelligent network interface providing protocol translation selected from any two protocols within a single layer of an ISO 7 layer protocol stack because IP and IPsec are both protocols in layer 3. Sun does not disclose that the information used by the routers to encrypt the packets is transmitted to the routers from the SMS using servlets. Lilja discloses updating the firmware of routers using plug-ins distributed over a network, where the firmware includes encryption functionality (Col. 3, lines 7-26), which meets the limitation of servlets because Applicant's specification defines servlets as plug-ins (Page 23, paragraph 81). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the routers' firmware in Sun defined by plug-ins transmitted from the SMS over the network in order to provide a more efficient means of updating the router firmware as discussed by Lilja (Col. 1, lines 42-67). Additionally, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the SMS to distribute these plug-ins because the SMS generates the cryptographic information (Sun: [0041]).

Referring to claims 4-6, 22, Sun discloses that each node in the network has a globally unique identifier ([0060]), which meets the limitation of a distinguished name. Sun further discloses that the routers are used to provide security services such as firewalls ([0037]), which meets the limitation of distinguished name firewall, and security patching. Sun does not disclose that the information used by the routers to encrypt the packets is transmitted to the routers from

Art Unit: 2132

the SMS using servlets. Lilja discloses updating the firmware of routers using plug-ins distributed over a network, where the firmware includes encryption functionality (Col. 3, lines 7-26), which meets the limitation of servlets because Applicant's specification defines servlets as plug-ins (Page 23, paragraph 81). It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the routers' firmware in Sun defined by plug-ins transmitted from the SMS over the network in order to provide a more efficient means of updating the router firmware as discussed by Lilja (Col. 1, lines 42-67). Additionally, it would have been obvious to one of ordinary skill in the art at the time the invention was made for the SMS to distribute these plug-ins because the SMS generates the cryptographic information (Sun: [0041]).

8. Claims 8, 10, 35 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sun, U.S. Publication No. 2002/0152373, in view of Elteto, U.S. Patent No. 7,111,324. Referring to claim 8, Sun does not specify any specific type of authentication information used in the network. Elteto discloses the user entering biometric information and PIN information using a token in a network environment (Col. 4, lines 16-24, 62-67), which meets the limitation of authentication includes biometric inputs, smart cards, tokens. It would have been obvious to one of ordinary skill in the art the time the invention was made to have the user input biometric or PIN information into a token in order to control access to network services as taught by Elteto (Col. 4, lines 35-36).

Referring to claims 10, 35, Sun discloses a tunnel interface for securing traffic over a network wherein each node in the network has a router between itself and the network (Figures 4 & 14), which meets the limitation of providing an intelligent network interface between a

Art Unit: 2132

network and each node on the network. The SMS provides IPsec public/private key generation for the nodes in the network ([0041]), which meets the limitation of providing a central management console on said network. Sun does not specify any specific type of authentication information used in the network. Elteto discloses the user entering biometric information and PIN information using a token in a network environment (Col. 4, lines 16-24, 62-67), which meets the limitation of a user providing a distinguished name and authentication to a first intelligent network interface attached to the user's host device, the first intelligent network interface verifying the user's authentication with the CMC such that when said user requests services from a second device. It would have been obvious to one of ordinary skill in the art the time the invention was made to have the user input biometric or PIN information into a token in order to control access to network services as taught by Elteto (Col. 4, lines 35-36). The IPsec communications are initialized by a first node ([0060]), which meets the limitation of the first intelligent network interface requests communication with said second device based on distinguished name. The SMS negotiates a logical ID to have a channel going between the two nodes ([0060]), which meets the limitation of said second intelligent network interface querying said CMC for permission and user authentication for the second device based on distinguished name. SMS negotiates a channel between two nodes having unique identifiers ([0060]). The SMS provides IPsec public/private key generation for the nodes in the network ([0041]), which meets the limitation of the CMC provides user authentication information based on distinguished name to said second intelligent network interface to allow said second intelligent network interface to log the user into the second device.



9. Claims 12-14, 17, 19, 20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sun, U.S. Publication No. 2002/0152373, in view of Ho, U.S. Patent No. 6,910,148. Referring to claims 12-14, 17, 20, Sun discloses that the routers are virtual routers equivalent to independent hardware routers ([0045]). It would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize hardware routers instead of the virtual routers proposed by Sun because in the event of a router failure, network utilizing hardware routers do not have the "glitch time" problem that networks utilizing virtual networks have, as taught by Ho (Col. 1, line 55 – Col. 2, line 34). Hardware routers would have a CPU, memory, I/O interface to the network, I/O interface to the node, and be considered a standalone device. The operating systems for the routers and nodes would be distinct because the routers are separate from the nodes.

Referring to claim 19, the combination of Sun, in view of Ho, does not specify having the operating system of the router stored on a hard drive. However, it would have been obvious to one of ordinary skill in the art at the time the invention was made to utilize a hard drive to store the operating system of the router in order to provide a large, non-volatile storage means for the operating system.

10. Claims 15-16 are rejected under 35 U.S.C. 103(a) as being unpatentable over Sun, U.S. Publication No. 2002/0152373, in view of Ho, U.S. Patent No. 6,910,148 as applied to claims 11-12 above, and further in view of Elteto, U.S. Patent No. 7,111,324. Referring to claim 15-16, Sun does not specify any specific type of authentication information used in the network. Elteto discloses the user entering biometric information and PIN information using a USB token in a network environment (Abstract & Col. 4, lines 16-24, 62-67), which meets the limitation of intelligent network interface further comprises a serial link authentication port, the serial line

Art Unit: 2132

authentication port is a USB port. It would have been obvious to one of ordinary skill in the art at the time the invention was made to have the user input biometric or PIN information into a token in order to control access to network services as taught by Elteto (Col. 4, lines 35-36).

11. Claim 18 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sun, U.S. Publication No. 2002/0152373, in view of Ho, U.S. Patent No. 6,910,148 as applied to claim 11-12 above, and further in view of Kitazaki, U.S. patent No. 6,172,936. Referring to claim 18, the combination of Sun, in view of Ho does not suggest a hardware router with an operating system in flash memory. Kitazaki discloses storing the operating system on a flash memory (Col. 1, line 60). It would have been obvious to one of ordinary skill in the art at the time the invention was made to store the operating system of the hardware router on a flash memory in order to obviate the need to transfer the operating system to main memory from the hard disk, which significantly reduces boot up time (Col. 1, lines 61-64).

12. Claim 21 is rejected under 35 U.S.C. 103(a) as being unpatentable over Sun, U.S. Publication No. 2002/0152373, in view of Ho, U.S. Patent No. 6,910,14 as applied to claim 11 above, and further in view of Walter, U.S. Patent No. 6,151,677. Referring to claim 21, the combination of Sun, in view of Ho, does not suggest that the router contains an encryption accelerator on an FPGA. Walter discloses encryption capabilities on an FPGA (Col. 7, lines 29-32). It would have been obvious to one of ordinary skill in the art at the time the invention was made to use an FPGA for encryption purposes in order to provide for inherent tamper protection of the encryption information (Walter: Col. 4, lines 55-63).

### ***Conclusion***

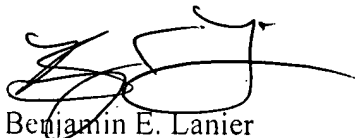
Art Unit: 2132

13. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Benjamin E. Lanier whose telephone number is 571-272-3805.

The examiner can normally be reached on M-Th 7:30am-5:00pm, F 7:30am-4pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.



Benjamin E. Lanier